UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/612,324	07/06/2000	James W. Edwards	10559-227001/P8792	7184

20985 7590 12/28/2006
FISH & RICHARDSON, PC
P.O. BOX 1022
MINNEAPOLIS, MN 55440-1022

EXAMINER	
COLIN, CARL G	
ART UNIT	PAPER NUMBER
2136	

SHORTENED STATUTORY PERIOD OF RESPONSE	MAIL DATE	DELIVERY MODE
3 MONTHS	12/28/2006	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

If NO period for reply is specified above, the maximum statutory period will apply and will expire 6 MONTHS from the mailing date of this communication.

Office Action Summary	Application No.	Applicant(s)	
	09/612,324	EDWARDS ET AL.	
	Examiner	Art Unit	
	Carl Colin	2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *06 October 2006*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-3,7-19,26-30,32-34,36 and 38* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-3, 7-19, 26-30, 32-34, 36, and 38* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Continued Examination Under 37 CFR 1.114

1. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 8/8/2006 has been entered.

Response to Arguments

2. In response to communications filed on 8/8/2006 and 10/6/2006, applicant amends claims 1, 11, 26, 33, 34, cancels claims 31, 35, and 37. The following claims 1-3, 7-19, 26-30, 32-34, 36, and 38 are presented for examination.

2.1 Applicant's remarks, pages 7-12, filed on 8/8/2006, with respect to the rejection of claims 11 and 53 have been fully considered, but they are not persuasive. Applicant argues that Richards fails to teach "establishing a first session between the source computer system and a forwarder/relay service wherein establishing the first session includes processing data to represent the data using a proxy network protocol so that the processed data is configured to tunnel through the first connectivity barrier" as amended. Applicant adds that Richards does not provide any detail regarding processing. It is noted that the independent claims as amended provide no details about the processing by merely stating processing data to represent data so

that the data is configured to go through the firewall. The claims as amended do not explicitly recite how the data is processed and what kind of processing is done. Examiner asserts that Richards discloses providing service to clients that cannot normally communicate to each other through the firewall (connectivity barrier) using network protocol TCP/IP, the nexus allows these clients to communicate through a secure connection where communications are sent and relayed to the appropriate client (see column 4, line 63- col. 5, line 10). Richards discloses the client resides behind a first connectivity barrier to establish communication with the nexus (forwarder/relay service). The nexus supports network protocol SSL and other encryption process, the SSL provides data encryption, server authentication, message integrity and client authentication for a TCP/IP connection (see column 5, lines 48-64). Therefore as interpreted by the Examiner when an SSL session is established between the client (behind a first connectivity barrier) and the nexus, the client is authenticated using TCP/IP and encryption protocols to establish a secure communication with the nexus, which meets the recitation of processing data using a network protocol to tunnel through the firewall. (See also column 6, lines 52-67 for another embodiment for handling client communication processing between the client and the nexus). In response to Applicant that Alkatib does not disclose a firewall, the gateway of Alkatib is used as a firewall (see column 1, lines 30-33) and meets the recitation of firewall as it controls access to the private network (see column 2, lines 3-8). The mapping disclosed by Alkatib meets also the recitation of processing data as explained in the rejection below. Applicant has not overcome the rejection in view of the cited prior art. The claims are still obvious over the prior art. Therefore, the claims remain rejected in view of the prior art.

Claim Objections

3. Claim 34 is objected to because the claim has been amended to replace a forward mode for communicating data using a network protocol to "communicating data without using a network protocol". The limitation of communicating data without using any proxy network protocol is not clear to the Examiner, it is understood that an e-mail relay/forwarding, address translation, transport protocol are all some type of network protocol used by a proxy application including SSL, HTTP, FTP, SOCKS, etc.. The address mode on page 8, lines 15-20 is believed by the Examiner to be a type of proxy network protocol. Appropriate correction or further clarification is required.

Claim Rejections - 35 USC § 103

4. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 1-3, 7-19, 32, and 36 are rejected under 35 U.S.C. 103(a) as being unpatentable over US Patent 6,754,707 to **Richards et al** in view of US Patent 6,421,732 to **Alkhatib et al** and in view of US Patent 5,564,070 to **Want et al**.

As per claim 1, Richards et al substantially discloses *a method of establishing communications comprising: establishing a virtual connection between a source computer system and located behind a first connectivity barrier* (firewall) *and a destination computer system and located behind a second connectivity barrier* (firewall), for example (see column 11, claim 1 and column 12, claim 14); *establishing a first session between the source computer system and a forwarder/relay service and establishing a second session between the destination computer system and the forwarder/relay service*, for example (see column 11, claim 1 and column 12, claim 14). See also column 4, line 55 through column 5, line 50. Richards discloses restoring previously working states from reference states in a transparent way (column 3, lines 42-61). **Richards et al** teaches "a nexus that allows client programs to communicate by acting as a central junction where communications are sent and relayed to the appropriate client programs... the nexus forwards communication on the destination's client registered downspout" and relaying information (see column 4, line 55 through column 5, line 50 and column 6, lines 10-15 and 35-46) that meets the recitation of *forwarder/relay service.* **Richards et al** further discloses the nexus supports network protocol SSL and other suitable encryption processes, the SSL provides data encryption, server authentication, message integrity and client authentication for a TCP/IP connection (see column 5, lines 48-64). Therefore as interpreted by the Examiner, **Richards et al** discloses encryption process and authentication using TCP/IP as part of

processed data to pass through the firewall. The passage above describes, when an SSL session is established between the client (behind a first connectivity barrier) and the nexus, the client is authenticated using TCP/IP and encryption protocols to establish a secure communication with the nexus, the browsers enable users to encrypt transaction, which meets the recitation of *wherein establishing the first session includes processing data to represent data using a proxy network protocol to tunnel through the first connectivity barrier* (firewall). (See also column 6, lines 52-67 for another embodiment for handling client communication processing between the client and the nexus). **Richards et al** also discloses establishing a virtual connection between two computers wherein a session between nexus and one of the computers remains open and even if the other computer connection is lost or interrupted the other computer re-establishes connection (see column 12, lines 42-45 and 63-67). **Richards et al** discloses maintaining the first session, but does not explicitly state maintaining the second session. It is apparent that any of the endpoint sessions can be maintained while the other endpoint connection is temporarily lost and re-establishing connection (e.g. roaming between networks). Roaming between networks is notoriously well known for a wireless to search between networks to reestablish sessions. Maintaining a connection to a destination endpoint when the source roams between network as the connection can be temporary lost is well known in the art as disclosed by **Want et al**. **Want et al** teaches maintaining connections among various computers in a wireless network including mobile computers, and further discloses the importance of maintaining connection even if the connection of the source endpoint is temporarily lost (see prior art, column 3, line 45 through column 4, line 55). See also column 7, lines 15-43. **Want et al** discloses that the application session is maintained even if the session with the mobile is temporarily lost as the

mobile re-establishes connection while roaming. Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the method of **Richards et al** to use source computer system as mobile users that can roam between networks and re-establish connection when the connection is temporarily lost while maintaining continuity session with the destination computer as taught by **Want et al** (column 7, lines 15-43) because one of the many advantages is that it permits any type of small device mobile units capable of roaming to use the system while maintaining processing continuity without compromising security (column 4, line 57 through column 5, line 40 and column 6, line 62 through column 7, line 43). One skilled in the art would have been motivated by the suggestions provided by **Want et al** in order to benefit from the advantages as discussed above and to be able to implement the invention with any mobile and stationary computers using various network systems.

Richards et al does not explicitly disclose *assigning virtual host name* to the computer system. It is known in the art that the packet can contain IP addresses and port numbers or/and domain names. **Alkhatib et al** in an analogous art teaches an IPNet gateway service that can forward and relay connections wherein the destination server is assigned a domain name (column 2, lines 53-60 and figure 1) and the client may have also a domain name (column 6, lines 37-47) so that address translation can be performed. **Alkhatib et al** also discloses the use of gateway as firewall (see column 1, lines 30-35), which meets the recitation of a barrier between a computer system and the gateway service as per Examiner's interpretation. Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the method of **Richards et al** to include a gateway service that can associate DNS requests with host names because it provides an improved process of addressing source and destination computers

based on the requests by performing address translation (column 1, lines 25-40 and column 1, line 60 through column 2, line 7) that can also be interpreted as processed data using a network protocol configured to tunnel through the gateway firewall as taught by **Alkhatib et al**. One skilled in the art would have been motivated by the suggestions provided by **Alkhatib et al** to provide a service that can forward and relay connections wherein the destination server is assigned a domain name with an improved process of addressing source and destination computers based on the requests by performing address translation.

As per claim 2, the references as combined above disclose the claimed method of claim 1. **Richards et al** discloses the limitation of wherein at least one of the connectivity barriers comprises a firewall, for example (see column 11, claim 1 and column 12, claim 14).

As per claim 3, the references as combined above disclose wherein at least one of the connectivity barriers comprises a consumer gateway (see **Alkhatib et al**, column 1, lines 32-33). Claim 3 is therefore rejected on the same rationale as the rejection of claim 1.

As per claims 7-8, the references as combined above disclose the claimed method of claim 1. **Alkhatib et al** discloses wherein the virtual host names comprise part of a hierarchical naming system, (column 3, lines 53-60) and discloses using a DNS that allows users to search for host names (column 3, line 45 through column 4, line 7) that meets the recitation of providing a directory search application to allow a user to select the virtual host names. Therefore claims 7-8 are rejected on the same rationale as the rejection of claim 1.

As per claim 9, the references as combined above disclose the claimed method of claim 1, wherein the source system can roam between networks (see **Want et al,** column 7, lines 15-43). Claim 9 is therefore rejected on the same rationale as the rejection of claim 1.

As per claim 10, the references as combined above disclose the claimed method of claim 1. **Richards et al** further discloses the limitation of including dynamically assigning at least one server associated with the service to handle the sessions, for example (see column 7, lines 27-48).

As per claim 11, **Richards et al** substantially discloses a method of establishing communications between source and destination computer systems comprising: *establishing a session between the source computer system located behind a first connectivity barrier and a service*, for example (see column 11, claim 1 and column 12, claim 14); and *establishing a transport level communications connection between the service and the destination computer system, the destination computer system located behind a second connectivity barrier*, for example (see column 11, claim 1 and column 12, claim 14). **Richards et al** teaches "a nexus that allows client programs to communicate by acting as a central junction where communications are sent and relayed to the appropriate client programs... the nexus forwards communication on the destination's client registered downspout" and relaying information (see column 4, line 55 through column 5, line 50 and column 6, lines 10-15 and 35-46) that meets the recitation of *forwarder/relay service.* **Richards et al** further discloses the nexus supports

network protocol SSL and other encryption process, the SSL provides data encryption, server authentication, message integrity and client authentication for a TCP/IP connection (see column 5, lines 48-64). Therefore as interpreted by the Examiner, **Richards et al** discloses encryption process and authentication using TCP/IP as part of processed data to pass through the firewall. The passage above describes, when an SSL session is established between the client (behind a first connectivity barrier) and the nexus, the client is authenticated using TCP/IP and encryption protocols to establish a secure communication with the nexus, the browsers enable users to encrypt transaction, which meets the recitation of *wherein establishing the first session includes processing data to represent data using a proxy network protocol to tunnel through the first connectivity barrier* (firewall). (See also column 6, lines 52-67 for another embodiment for handling client communication processing between the client and the nexus).

Richards et al discloses transport layer protocol such as TCP/IP connection can be used to establish communication between client/server using latest web browsers such as Netscape known to support HTTP, FTP, etc. (column 5, lines 43-65 and column 1, lines 56-64) that meets the recitation of *establishing a transport level communications between the forwarder/relay service and the destination computer system located behind a second connectivity barrier* (firewall). **Richards et al** also discloses establishing a virtual connection between two computers wherein a session between nexus and one of the computers remains open and even if the other computer connection is lost or interrupted the other computer re-establishes connection (see column 12, lines 42-45 and 63-67). **Richards et al** discloses maintaining the first session, but does not explicitly state maintaining the second session. It is apparent that any of the endpoint sessions can be maintained while the other endpoint connection is temporarily lost and

re-establishing connection (e.g. roaming between networks). Roaming between networks is notoriously well known for a wireless to search between networks to reestablish sessions. Maintaining a connection to a destination endpoint when the source roams between network as the connection can be temporary lost is well known in the art as disclosed by **Want et al**. **Want et al** teaches maintaining connections among various computers in a wireless network including mobile computers, and further discloses the importance of maintaining connection even if the connection of the source endpoint is temporarily lost (see prior art, column 3, line 45 through column 4, line 55). See also column 7, lines 15-43. **Want et al** discloses that the application session is maintained even if the session with the mobile is temporarily lost as the mobile re-establishes connection while roaming. Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the method of **Richards et al** to use source computer system as mobile users that can roam between networks and re-establish connection when the connection is temporarily lost while maintaining continuity session with the destination computer as taught by **Want et al** (column 7, lines 15-43) because one of the many advantages is that it permits any type of small device mobile units capable of roaming to use the system while maintaining processing continuity without compromising security (column 4, line 57 through column 5, line 40 and column 6, line 62 through column 7, line 43). One skilled in the art would have been motivated by the suggestions provided by **Want et al** in order to benefit from the advantages as discussed above and to be able to implement the invention with any mobile and stationary computers using various network systems.

For additional support, Applicant's amendment is also rendered obvious by **Alkhatib et al**. **Alkhatib et al** in an analogous art teaches an IPNet gateway service that can forward and

relay connections wherein the destination server is assigned a domain name (column 2, lines 53-60 and figure 1) and the client may have also a domain name (column 6, lines 37-47) so that address translation can be performed. **Alkhatib et al** also discloses the use of gateway as firewall (see column 1, lines 30-35), which meets the recitation of a barrier between a computer system and the gateway service as per Examiner's interpretation. Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the method of **Richards et al** to include to include a gateway service that can associate DNS requests with host names because it provides an improved process of addressing source and destination computers based on the requests by performing address translation (column 1, lines 25-40 and column 1, line 60 through column 2, line 7) that can also be interpreted as processed data using a network protocol configured to tunnel through the gateway firewall as taught by **Alkhatib et al**. One skilled in the art would have been motivated by the suggestions provided by **Alkhatib et al** to provide a service that can forward and relay connections wherein the destination server is assigned a domain name with an improved process of addressing source and destination computers based on the requests by performing address translation.

As per claim 12, the references as combined above disclose the claimed method of claim 11. **Richards et al** further discloses the limitation of wherein at least one of the connectivity barriers comprises a firewall, for example (see column 11, claim 1 and column 12, claim 14).

As per claim 13, Richards et al is silent about the firewalls comprising consumer gateways such as (router) which is a well known feature. **Alkhatib et al** discloses the use of

gateway as firewall (see column 1, lines 30-35). Claim 13 is rejected on the same rationale as the rejection of claim 11 above.

As per claim 14, the references as combined above disclose the claimed method of claim 11. **Richards et al** further discloses the limitation of including assigning one or more servers associated with the service to handle the sessions, for example (see column 7, lines 27-48).

As per claim 15, the references as combined above disclose establishing session based on a virtual host name associated with the source computer system (see **Alkhatib et al**, column 6, lines 37-47). Claim 13 is also rejected on the same rationale as the rejection of claim 11.

As per claims 16-17, Alkhatib et al discloses wherein the virtual host names comprise part of a hierarchical naming system, (column 3, lines 53-60) and discloses using a DNS that allows users to search for host names (column 3, line 45 through column 4, line 7) that meets the recitation of providing a directory search application to allow a user to select the virtual host names. Therefore claims 16-17 are rejected on the same rationale as the rejection of claim 11.

As per claim 18, the references as combined above disclose the claimed method of claim 11, wherein the source system can roam between networks (see **Want et al,** column 7, lines 15-43). Claim 18 is therefore rejected on the same rationale as the rejection of claim 11.

As per claim 19, Richards et al discloses the limitation of including dynamically assigning at least one server associated with the service to handle the sessions, for example (see column 7, lines 27-48).

As per claim 32, the combined references disclose the limitation of wherein the proxy network protocol includes at least one of HTTP, FTP, and SOCKS (see **Richards et al,** column 5, lines 43-65). **Richards et al** discloses transport layer protocol such as TCP/IP connection between client/server communication using latest web browsers such as Netscape known to support HTTP, FTP, etc. as interpreted by Examiner.

As per claim 36, the combined references disclose the limitation of wherein the proxy network protocol includes at least one of HTTP, FTP, and SOCKS (see **Richards et al,** column 5, lines 43-65). **Richards et al** discloses transport layer protocol such as TCP/IP connection between client/server communication using latest web browsers such as Netscape known to support HTTP, FTP, etc. as interpreted by Examiner.

5. **Claims 33-34** are rejected under 35 U.S.C. 103(a) as being unpatentable over US Patent 6,754,707 to **Richards et al** in view of US Patent 6,421,732 to **Alkhatib et al** and in view of US Patent 5,564,070 to **Want et al** as applied to claim 1 and further in view of US Patent 6,185,606 to **Bereiter**.

As per claim 33, Richards et al does not explicitly disclose making a determination of the communication node of the destination computer system. **Bereiter** in an analogous art teaches wherein establishing the second session comprises determining a communication mode for communicating between the destination computer system and the forward/relay service and communicating data between the destination computer system and the forward/relay service according to the determined communication mode (see Bereiter, column 4, lines 3-23 and column 4, line 51 through column 5, line 14). **Bereiter** discloses a communication method to adapt to different mode of communication depending on the connection preferences. For instance, a transport layer point-to-point protocol connection may be used for messages originating from the client to the server whereas another connection preference is used for messages originating from the server to the client that meets the recitation above. Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the method as combined above to determine the communication mode of the destination computer system and communicating data between the destination computer system and the forward/relay service according to the determined communication mode as taught by **Bereiter**. One skilled in the art would have been motivated by the suggestions provided by **Bereiter** so as to provide the benefit to adapt to the available communication path.

As per claim 34, Bereiter discloses using e-mail for a message originating at the server as a connection preference (see column 15-23 and column 5, lines 1-3); as interpreted herein, an e-mail is typically relayed through several servers using UDP that meets the recitation of wherein the communication mode includes at least one of a forward mode for communicating

data without using any proxy network protocol and a relay mode for communicating data using another proxy network protocol. Therefore claim 34 is rejected on the same rationale as the rejection of claim 33.

6. **Claims 26 and 38** are rejected under 35 U.S.C. 103(a) as being unpatentable over US Patent 6,754,707 to **Richards et al** in view of US Patent 5,564,070 to **Want et al**.

As per claim 26, Richards et al substantially discloses *an article comprising a computer-readable medium including computer-executable instructions for causing a computer system*, (see column 11, lines 9-18) *in response to a request from a first computer system located behind a first connectivity barrier to establish connectivity to a second computer system*, for example (see column 11, claim 1 and column 12, claim 14) *to: assigning a server to handle a first session between the first computer system and a service,* for example (see column 7, lines 27-48). and further teaches *establish a session initiated by the second computer system if the second computer system is located behind a second connectivity barrier*, for example (see column 4, line 63 - column 5, line 10). **Richards et al** teaches "a nexus that allows client programs to communicate by acting as a central junction where communications are sent and relayed to the appropriate client programs... the nexus forwards communication on the destination's client registered downspout" and relaying information (see column 4, line 55 through column 5, line 50 and column 6, lines 10-15 and 35-46) that meets the recitation of *forwarder/relay service.* **Richards et al** further discloses the nexus supports network protocol SSL and other encryption process, the SSL provides data encryption, server authentication,

message integrity and client authentication for a TCP/IP connection (see column 5, lines 48-64). Therefore as interpreted by the Examiner, **Richards et al** discloses encryption process and authentication using TCP/IP as part of processed data to pass through the firewall. The passage above describes, when an SSL session is established between the client (behind a first connectivity barrier) and the nexus, the client is authenticated using TCP/IP and encryption protocols to establish a secure communication with the nexus, the browsers enable users to encrypt transaction, which meets the recitation of *wherein establishing the first session includes processing data to represent data using a proxy network protocol to tunnel through the first connectivity barrier* (firewall). (See also column 6, lines 52-67 for another embodiment for handling client communication processing between the client and the nexus).

Richards discloses transport layer protocol such as TCP/IP connection can be used to establish communication between client/server using latest web browsers such as Netscape known to support HTTP, FTP, etc. (column 5, lines 43-65 and column 1, lines 56-64) that meets the recitation of *establishing a transport level communications between the forwarder/relay service and the destination computer system located behind a second connectivity barrier* (firewall). **Richards et al** also discloses establishing a virtual connection between two computers wherein a session between nexus and one of the computers remains open and even if the other computer connection is lost or interrupted the other computer re-establishes connection (see column 12, lines 42-45 and 63-67). **Richards et al** discloses maintaining the first session, but does not explicitly state maintaining the second session. It is apparent that any of the endpoint sessions can be maintained while the other endpoint connection is temporarily lost and re-establishing connection (e.g. roaming between networks). Roaming between networks is

notoriously well known for a wireless to search between networks to reestablish sessions. Maintaining a connection to a destination endpoint when the source roams between network as the connection can be temporary lost is well known in the art as disclosed by **Want et al**. **Want et al** teaches maintaining connections among various computers in a wireless network including mobile computers, and further discloses the importance of maintaining connection even if the connection of the source endpoint is temporarily lost (see prior art, column 3, line 45 through column 4, line 55). See also column 7, lines 15-43. **Want et al** discloses that the application session is maintained even if the session with the mobile is temporarily lost as the mobile re-establishes connection while roaming. Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the method of **Richards et al** to use source computer system as mobile users that can roam between networks and re-establish connection when the connection is temporarily lost while maintaining continuity session with the destination computer as taught by **Want et al** (column 7, lines 15-43) because one of the many advantages is that it permits any type of small device mobile units capable of roaming to use the system while maintaining processing continuity without compromising security (column 4, line 57 through column 5, line 40 and column 6, line 62 through column 7, line 43). One skilled in the art would have been motivated by the suggestions provided by **Want et al** in order to benefit from the advantages as discussed above and to be able to implement the invention with any mobile and stationary computers using various network systems.

As per claim 38, the combined references disclose the limitation of wherein the proxy network protocol includes at least one of HTTP, FTP, and SOCKS (see **Richards et al,** column

5, lines 43-65). **Richards et al** discloses transport layer protocol such as TCP/IP connection between client/server communication using latest web browsers such as Netscape known to support HTTP, FTP, etc. as interpreted by Examiner.

7. **Claims 27-28** are rejected under 35 U.S.C. 103(a) as being unpatentable over US Patent 6,754,707 to **Richards et al** in view of US Patent 5,564,070 to **Want et al** as applied to claim 26 and further in view of US Patent 6,185,606 to **Bereiter**.

As per claims 27-28, Richards et al discloses instructions for causing the computer system (nexus) to establish a transport level communications connection to the second computer system regardless of whether a firewall exists in the first computer system (see column 5, lines 1-10 and column 4, lines 63-67), the operations of Richards et al can be applied with or without firewall (see column 3, lines 43-51). **Richards et al** does not explicitly disclose making a determination in response to if the second computer system is not located behind a connectivity barrier (firewall). **Bereiter** in an analogous art teaches a system to establish a session initiated by the second computer system if the second computer system is located behind a second connectivity barrier and to instruct the first computer system to establish a direct session or transport level communications connection with the second computer system if the second computer system is not located behind a connectivity barrier to adapt to the available communication path, for example (see column 3, line 40 through column 4, line 23). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the method of **Richards et al** to establish a session initiated by the second computer

system if the second computer system is located behind a second connectivity barrier and to instruct the first computer system to establish a direct session with the second computer system if the second computer system is not located behind a connectivity barrier in order to adapt to the available communication path as taught by **Bereiter**. One skilled in the art would have been motivated by the suggestions provided by **Bereiter** so as to provide the benefit to adapt to the available communication path.

8. **Claims 29-30** are rejected under 35 U.S.C. 103(a) as being unpatentable over US Patent 6,754,707 to **Richards et al** in view of US Patent 5,564,070 to **Want et al** as applied to claim 26 and further in view of US Patent 6,421,732 to **Alkhatib et al**.

As per claim 29, Richards et al does not explicitly disclose *assigning virtual host name* to the computer system. It is known in the art that the packet can contain IP addresses and port numbers or/and domain names. **Alkhatib et al** in an analogous art teaches an IPNet gateway service that can forward and relay connections wherein the destination server is assigned a domain name (column 2, lines 53-60 and figure 1) and the client may have also a domain name (column 6, lines 37-47) so that address translation can be performed. Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the method as combined above to include a gateway service that can associate DNS requests with host names because it provides an improved process of addressing source and destination computers based on the requests by performing address translation (column 1, lines 25-40 and column 1, line 60 through column 2, line 7) as taught by **Alkhatib et al**. One skilled in the art

would have been motivated by the suggestions provided by **Alkhatib et al** to provide a service that can forward and relay connections wherein the destination server is assigned a domain name with an improved process of addressing source and destination computers based on the requests by performing address translation.

As per claim 30, Alkhatib et al discloses wherein the virtual host names comprise part of a hierarchical naming system, (column 3, lines 53-60). Therefore claim 30 is also rejected on the same rationale as the rejection of claim 29.

Conclusion

9. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Carl Colin whose telephone number is 571-272-3862. The examiner can normally be reached on Monday through Thursday, 8:00-6:30 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Nasser G. Moazzami can be reached on 571-272-4195. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would

like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Carl Colin
Patent Examiner
December 21, 2006